California Department of Motor Vehicles Bonded Web User Security Requirements

Business Name		CADMV USE ONLY	
Facility Address			
Inventory Address		Date Received	
BWU Program Admin		Date Reviewed	
ISO Analyst		☐ Approved	☐ Pending

I. Entities requesting receipt of California Department of Motor Vehicles (CADMV) information must have all requisite security requirements and features in place before application approval of the Bonded Web User (BWU) can be given. Additional information may be required to determine if specific security requirements have been implemented by the BWU.

II. Use only the electronic version of this form to respond. *Please note that every "No" response requires a target date response to indicate when compliance with the requirement is anticipated.*

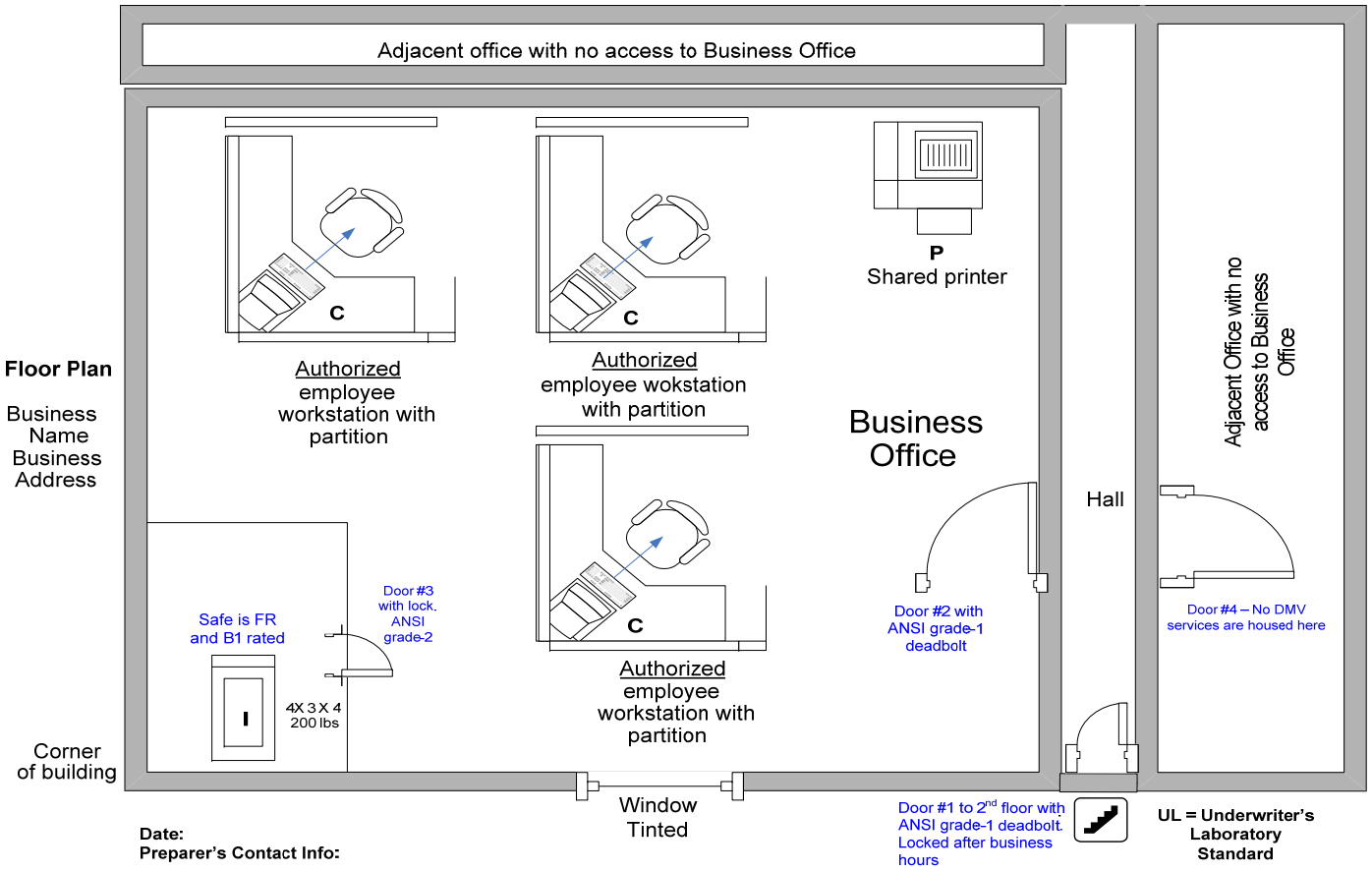
III. Business Facility Diagram (See Sample on page 2)

Provide a diagram of your business facility with the following details

- External & internal
  - o Doors
  - o Walls
  - o Windows and other openings
- The placement of
  - o Rooms/offices
  - o Counters
  - o Partitions
  - o Desks/ Workstations
  - o Location of CADMV Inventory storage
  - o Customer waiting areas

Use this legend for the following items on your diagram	
C →	Indicates the location of **C**omputers. The arrow (→) indicates the direction the monitor screen is facing.
P	Indicates the location of **P**rinters.
I	Indicates the location of CADMV **I**nventory storage (cabinet/safe) *after* business hours.
W	Indicates the location of CADMV Inventory storage (desk drawer/cabinet, etc.) *during* business (**w**ork) hours, if applicable.
All accountable and controlled inventories are required to be stored in an approved metal safe or cabinet after business hours.	
"Accountable inventory" is defined as apportioned license plates and apportioned year stickers.	
"Controlled inventory" is defined as CVRA weight decals/year stickers.	

Sample Diagram



California Department of Motor Vehicles Bonded Web User Security Requirements

Business Name		Date Reviewed			
	Bonded Web User Program Agreement	**PHYSICAL SECURITY REQUIREMENTS**	**Y**	**N**	**DATE**
1	The Bonded Web User shall implement the physical security measures and methods stated in this Agreement to prevent and discourage inadvertent or deliberate alteration, disclosure, destruction, loss, misuse, or theft of the CADMV records, and proprietary assets under their control.	**1.** Bonded Web User has **implemented** all requisite security measures and methods stated in this agreement to protect all CADMV records and proprietary assets under their control.	☐	☐	
2	The Bonded Web User shall be responsible for making sure it prevents access to CADMV records (retained in any portable medium or method), and proprietary assets by the general public and other unauthorized individuals.	**2.** Bonded Web User assumes the responsibility to prevent unauthorized **access and viewing** of CADMV records and proprietary assets.	☐	☐	
3	The Bonded Web User shall prevent the unauthorized viewing of CADMV proprietary assets displayed by any medium or method.				
4	The Bonded Web User shall provide a secure business site or facility. Business site or facility entries shall be equipped with doors or closures that are of solid construction and are equipped with positive locking devices such as dead bolt type locks. The Bonded Web User shall secure all external windows, skylights, and vents to the business site or facility in such a manner as to prevent entry and preclude viewing into any area of the business site or facility where CADMV proprietary assets are stored. The Bonded Web User shall also have a functioning camera and a functioning alarm for site surveillance. All surveillance equipment must be maintained and periodically checked to ensure continual operation. Videos capturing activity must be viewed and maintained to ensure operability. In addition, videos of site surveillance must be stored and rotated with a recommended time frame of six (6) months.	**3.** Facility entry doors or closures are of solid **construction** (e.g., tempered glass & metal frame, solid wood, or steel, etc.)	☐	☐	
		4. Facility doors are **equipped** with positive locking devices such as mortise and latch; lever, or dead bolt locks that meet ANSI/BHMA Grade-1 standards.	☐	☐	
		5. Facility external windows, skylights, and vents are **secured** in such a manner as to prevent unauthorized entry or viewing into areas where CADMV proprietary assets are stored.	☐	☐	
		6. The business facility is **equipped** with a functioning camera and alarm for site surveillance.	☐	☐	
		7. Video capturing and equipment are periodically **checked** to ensure operability.	☐	☐	
		8. Site surveillance videos are **stored** and **rotated** every six (6) months.	☐	☐	
		9. A completed **copy** of the *Physical Key Management Controls* for our entity is **attached**. BWU-Approved Key-Mgmt Policy.docm	☐	☐	

California Department of Motor Vehicles Bonded Web User Security Requirements

Business Name		Date Reviewed			
	Bonded Web User Program Agreement	**PHYSICAL SECURITY REQUIREMENTS**	**Y**	**N**	**DATE**
5	The Bonded Web User shall not leave CADMV proprietary assets retained in any portable medium or method under their control unattended when not secured on a device or location specified by this Agreement.	**10.** CADMV proprietary assets are not left unattended at anytime when not retained in an appropriate secure device or location.	☐	☐	
6	The Bonded Web User shall secure CADMV proprietary assets retained in any portable medium or method, under their control in a safe or cabinet of metal construction that is built into, or is permanently attached to, the business site or facility, unless the safe or cabinet is of sufficient size (at least four (4) feet in height or width) or weight (at least one hundred fifty (150) pounds to substantially preclude it from being readily removed from the business site or facility, during non-business hours. The safe or cabinet shall be equipped with a positive locking device(s) and the Bonded Web User shall restrict and control knowledge of, and use of, the method for unlocking the device to the individuals that have completed and signed an *Information Security and Disclosure Statement, Public and Private Partnerships Employee* form (EXEC 200X), which is incorporated by reference and made part of this Agreement submitted during the application process for participation in the Bonded Web User Program.	**11.** During **non-business hours** CADMV proprietary assets are secured in a safe or cabinet of metal construction meeting the following specifications:	☐	☐	
		(a) The safe or cabinet is at least 4-ft high or 4-ft wide, and weighs at least 150 pounds when empty.	☐	☐	
		(b) If the safe or cabinet is **not** of sufficient size or weight it is permanently attached (bolted) to a wall or floor of the business facility.	☐	☐	
		(c) The safe or cabinet is equipped with a positive locking device (combination pad, padlock, cabinet lock).	☐	☐	
		(d) Knowledge of and the method for unlocking the safe or cabinet is restricted to authorized individuals that have completed and signed the EXEC200X form.	☐	☐	
7	The Bonded Web User shall secure CADMV proprietary assets retained in any portable medium or method under their control during business hours in a device that is not readily portable (e.g., in a large metal cabinet, desk, or workstation drawer) and is equipped with a positive locking device. The Bonded Web User shall implement physical barriers that prevent the general public and other unauthorized individuals from having access to the secured storage device and restrict and control the knowledge of, and use of, the method for unlocking the device to individuals that have completed and signed an EXEC 200X form.	**12.** During **business hours:** (a) CADMV proprietary assets are secured in a large metal cabinet, desk or workstation drawer equipped with a positive locking device.	☐	☐	
		(b) Physical barriers are implemented to prevent unauthorized access of secure storage device(s).	☐	☐	

California Department of Motor Vehicles Bonded Web User Security Requirements

Business Name		Date Reviewed			
	Bonded Web User Program Agreement	**PHYSICAL SECURITY REQUIREMENTS**	**Y**	**N**	**DATE**
8	The Bonded Web User shall not transfer, retain, or store any CADMV records on any portable electronic medium such as diskettes, CD-ROMs, removable memory chips, or magnetic tapes.	**13.** CADMV records are NOT retained or stored on portable electronic media; such as, but not limited to CDs, DVDs, removable chips, USB devices, or magnetic tapes.	☐	☐	
9	The Bonded Web User shall be responsible for the disposal and destruction of specified proprietary assets and records as authorized by the CADMV in this Agreement in the manner authorized by CADMV for records created or maintained in the performance of this Agreement, and retained in either hardcopy format or electronic memory medium. Hardcopy records shall be shredded or made unusable. Electronic records shall be electronically "deleted" from the medium. All records subject to disposal or destruction by the Bonded Web User shall be completely rendered unreadable, unrecoverable, and unusable.	**14.** CADMV proprietary assets and records (hardcopy and electronic) are appropriately disposed and destroyed, as authorized by CADMV. Disposed CADMV assets and records are rendered completely unreadable, unrecoverable, and unusable.	☐	☐	
	Bonded Web User Program Agreement	**COMPUTER SYSTEM SECURITY REQUIREMENTS**	**Y**	**N**	**DATE**
1	The Bonded Web User shall place network and system devices used in the Bonded Web User Program and CADMV interface in secure areas. The Bonded Web User shall control access to these devices and shall limit access to, and viewing of (if appropriate) these devices to individuals that have completed and signed an *Information Security and Disclosure Statement, Public and Private Partnerships Employee* form (EXEC 200X) submitted during the application process for participation in the Bonded Web User Program.	**15.** Workstation components (PC, monitors, and printers) are placed in secure areas. Access and viewing of workstation components is limited to authorized employees who have completed and signed the EXEC200X form.	☐	☐	
2	The Bonded Web User shall require workstations and printers utilized to access the CADMV IRP vehicle registration and inventory databases and display or print CADMV records, be located within the Bonded Web User's site or facility in such a manner that displayed or printed records are not visible or accessible to unauthorized employees or the general public.	**16.** The location and placement of workstation components are such that displayed records are not visible or accessible to unauthorized employees or the general public within a distance of 10-feet.	☐	☐	
3	Workstations displaying CADMV records or the CADMV's IRP vehicle registration and titling or inventory database information shall display an electronic "admonishment warning banner" to the user at the time of accessing information. The banner shall contain the following language: "WARNING: Unauthorized access or misuse of data may result in disciplinary action, civil penalties and/or criminal prosecution."	**17.** Workstations displaying CADMV records or IRP inventory database information display an electronic admonishment warning banner to each user as the time of access. The banner contains the following language: "*WARNING: Unauthorized access or misuse of data may result in disciplinary action, civil penalties and/or criminal prosecution."*	☐	☐	

California Department of Motor Vehicles Bonded Web User Security Requirements

Business Name		Date Reviewed			
	Bonded Web User Program Agreement	**COMPUTER SYSTEM SECURITY REQUIREMENTS**	**Y**	**N**	**DATE**
4	Workstations shall not be left unattended while accessing the CADMV vehicle registration and inventory database. Workstations shall be configured to either programmatically end access or invoke a display obfuscation screen after a maximum of ten (10) continuous minutes of inactivity. Once access has ended or the display screen has been obfuscated, the user shall be required to re-authenticate to the authentication credentialing system prior to re-establishing access or un-obscuring the display.	**18.** Workstations are configured to programmatically end access or obfuscate the screen after 10 minutes of continuous inactivity; after which time the user is required to re-authenticate to re-establish access.	☐	☐	
	OTHER CADMV REQUIREMENTS	**PROPRIETARY ASSETS REQUIREMENTS**	**Y**	**N**	**DATE**
1	No "working" inventories of CADMV items *(accountable and controlled inventory)* are to be maintained outside of the permanent secure storage device during non-business hours. All CADMV inventories are to be kept in the device that you previously designated and described in the Business Facility Diagram.	**19.** All CADMV proprietary assets are kept in the designated storage device, of required dimensions and weight, during non-business hours.	☐	☐	
2	Obsolete and damaged CADMV inventory must be recorded with CADMV before it is destroyed. The method of destruction must ensure that the CADMV inventory item is rendered unusable, unreadable, and unrecoverable.	**20.** Obsolete and damaged inventory is recorded with CADMV before it is appropriately destroyed.	☐	☐	
3	No CADMV information shall be electronically stored away from the CADMV computer system. No customer private or confidential information such as residence address shall be kept on the computer hard drive, or via any portable recording methods.	**21.** No CADMV information is electronically stored on the computer hard drive, any portable medium, or away from the CADMV computer system.	☐	☐	
4	All CADMV paperwork shall be destroyed after legitimate business use has ended. The method of destruction (i.e., shredding) shall ensure that the information contained on the paperwork is rendered unusable, unreadable, and unrecoverable.	**22.** All paper documents containing CADMV data are appropriately destroyed after the legitimate business use has ended.	☐	☐	
5	All employees with direct or incidental access to CADMV computers, printers, and inventory items, must complete and sign an *Information Security and Disclosure Statement, Public and Private Partnership Employee* form (EXEC200X), at the time of hire or the granting of access, and annually thereafter for as long as access is authorized. The form must be maintained for three (3) years following each removal or expiration of an individual's access authorization, and be available, upon written request to CADMV.	**23.** Employees with direct or incidental access to CADMV proprietary assets will complete and sign the EXEC200X information security disclosure statement at the time of hire or granting of access, and **annually** thereafter. **24.** The EXEC200X is available to CADMV for 3 years after removal or expiration of an individual's access authorization, upon written request.	☐ ☐	☐ ☐	

California Department of Motor Vehicles Bonded Web User Security Requirements

Business Name		Date Reviewed			
	IRP and VC § REQUIREMENTS	**RECORDS RETENTION REQUIREMENTS**	**Y**	**N**	**DATE**
1	International Registration Plan §1005 1005 PRESERVATION AND AVAILABILITY OF RECORDS (a) The Base Jurisdiction shall require a Registrant to preserve all Operational Records on which the Registrant's application for apportioned registration is based for a period of 3 years following the close of the Registration year to which the application pertains and to make these records available for examination by the Base Jurisdiction at its request. (b) Records may be kept on microfilm, microfiche, or other computerized or condensed record storage system acceptable to the Base Jurisdiction. http://www.irponline.org/irp/DocumentDisplay.aspx?id={A29DF743-0456-40D9-933C-EABD9EBEA0C4}	**25.** Operational and Fleet Records may be securely stored on microfilm, microfiche, or other computerized or condensed record storage system for the periods of time specified by IRP §1005, and VC § 8057.	☐	☐	
2	Vehicle Code § 8057 8057**.** Any person issued fleet registration pursuant to Article 9.5 (commencing with Section 5301) of Chapter 1 or this article shall: (a) Maintain fleet records that support the reported mileage, cost, and declared gross or combined gross **vehicle** weight of all vehicles. Any registrant whose application for apportioned registration has been accepted shall preserve the mileage records on which the application is based, including copies of all permits, for a period of three years after the close of the registration year. **Vehicle** cost and declared gross or combined gross weight records shall be retained for four years after the close of the registration year in which the **vehicle** was deleted. (b) Make fleet records available to the department at its request for audit to verify the accuracy of the records. In the event the records are not made available within 30 days of the request, the department may assess full California fees and penalties and may suspend or cancel apportioned registration privileges. The registrant may be required to reimburse the department auditor per diem and travel expenses under certain conditions as determined by the director.	**26.** Access controls are in place to restrict the unauthorized access and viewing of stored Operational and Fleet Records. **27.** Operational and Fleet Records shall be made available for examination upon the request of CADMV	☐ ☐	☐ ☐	

All answers provided in this document, and any and all activities undertaken pursuant to the BWU Program, may be verified during an audit, inspection, or investigation by Department of Motor Vehicles personnel, representatives, or law enforcement. Any discrepancies found during the course of any such audit, inspection or investigation may be grounds for suspension or termination from the BWU Program.

As a prerequisite for participation in the BWU Program, the undersigned represents and affirms that any errors discovered in connection with involvement or participation in the BWU Program will be immediately brought to the attention of the BWU Program Administrators.

I certify (or declare) under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

BWU Authorized Representative: _____ Date: _____

(Signature)